Sparse Encoded Matrix based Steganography algorithm

Vipul Shah

M.E. Student, Department Of Computer Science, J.N. University, Jodhpur-340021

---***---

Abstract-*Image steganography is a field of steganography where images are used to hide information. Nowadays with the increasing lack of security online it is important to have means to make our data safe. In this paper we propose a method to increase the security of our data by means of steganography. We use a sparse encoded matrix to encode our information such as the key and data and this helps to increase the security of the algorithm. On further inspection we can see that the algorithm gives great results and can be used for practical purposes.*

***Key Words*: Steganography, sparse matrix, security**

1.INTRODUCTION

Over the years the lack of information security has led to leakage of private information. A lot of recent developments has happened in the field of cryptography [1]. Still there has been no decrease in the rate of cyber crime.

Some of the recent developments in cryptography have seen modifications to older algorithms. For example [2] was a modification of the Caesar Cipher algorithm and has been seen to increase the efficiency of the algorithm by enhancing the security without changing the speed too much of the algorithm.

There has been a shift from mainstream cryptography to field such as lattice cryptography and elliptic cryptography. Lattice based cryptography is the utilization of conjectured hard problems on point lattices [3]. This type of cryptography has been seen to increase the security of the standard cryptography algorithms and hence is being preferred.

Cryptography has found applications in the wireless sensor domain [4]. This helps to secure information over insecure media as the information gets transmitted. Although cryptography gives good strength to the algorithm there is still lot to be desired over the increasing lack of security provided.

Cryptography is the technique of keeping information secured by converting text of one form into another. When somebody sees this new form of text it raises a doubt in their eyes and hence the evolution of steganography. Steganography helps to keep the information secure whilst at the same time preventing the knowledge of information being hidden from being leaked.

However latest developments give some positive hope with regards to cryptography being strong enough by itself [5].

Recently the strongest cryptography algorithm was broken down by means of a super computer. So there is still some time for cryptography to show it can be used as the sole form of security.

Latest research shows the development of leakage resistant algorithms [6]. They solve the issue of leakage itself instead of making the algorithm stronger. This way the security is enhanced as the leakage of information is much harder for anybody to crack.

The rest of the paper is organized as: Related work (which talks about recent developments in the field of steganography and how those developments have helped to strengthen security), Proposed work (which gives an explanation of the proposed algorithm and the steps involved in making it), experimental analysis (which gives a comparitive analysis of the algorithm with the likes of the least significant bit algorithm among others, LSB is used because it is the most popular algorithm around for image steganogrpahy) and the conclusion of the proposed work.

2. RELATED WORK

Steganography is a technique of hiding information where the idea that information is being hidden is not known to any eavesdropped no matter how smart he may be.

Some simple steganography algorithms include the use of facebook to hide information [7]. In this they use cover images of a person to hide information and share it with particular set of people. This is very hard to identify as the fact that information is being hidden is known only to the people who are sharing that image with each other. Also facebook provides additional security information to prevent strangers from seeing your photos and this adds to the security of using facebook as a medium.

Another method to increase security of steganographic methods is to make your algorithm more random as it will increase the chaos factor of the algorithm. Breaking down of text into blocks and sending them in random order helps to increase the chaos factor due to the random nature of sending of the blocks [8].

Sometimes using cryptography with steganography has been seen to increase the security of the algorithms. Many such methods have been proposed. In [9] DWT was used with Lorenz encryption and visual cryptology. This gave 3 layers of security to the proposed algorithm and made it very difficult to crack down.

A universal function was developed in [10] that gave distortion in a random or arbitrary domain and this caused to increase the security of the algorithm. Results showed that the algorithm did better than most recent algorithms.

In [11] an algorithm was developed which was content adaptive i.e the algorithm adapted on the basis of the proposed content. This was done along with decreasing statistically detectability and the results showed great increase in security. This is considered one of the state of the art approaches to steganography.

In [12] the use of universal distortion was proposed and it was seen that the algorithm gave great results.

Another algorithm that used combination of Cryptography and steganography algorithms was proposed in [13]. Here the use of blowfish algorithm increased the security of the information before even hiding it actually.

In [14] the authors proposed content adaptive pentary steganography algorithm that used multivariate generalized Gaussian cover model to execute. Again since this was a content adaptive algorithm it gave great results in terms of execution and accuracy.

3. PROPOSED WORK

The proposed approach is explained as follows,

Step 1: Obtain information to hide

Step 2: Obtain Cover image

Step 3: Use sparse-matrix encoding on information to be hidden and store that matrix

Step 4: Expand matrix by considering it be equal size of image and scale it
Step 5: Use LSB to embed information of each bit into the image
Step 6: Stop

The proposed approach uses a sparse encoding matrix to hide the information before encoding it. This increases security of the information and for that purpose it is highly recommended to do the same.

3. EXPERIMENTS

The experiments were done in comparison with the Least Significant bit algorithm. We tested the time needed for our algorithm to execute and compare the same with standard algorithm.
Next we tested the amount of data that could be hidden by first our approach and second that of the standard approach.
Table 1 is time comparison and table 2 is PSNR comparison.

Table -1: Time comparison

Time Comparison			
Proposed (Text size = 1 kb)	0.51 seconds	LSB (Text size = 1 kb)	0.50 seconds
Proposed (Text size = 10 kb)	1.27 seconds	LSB (Text size = 10 kb)	1.26 seconds
Proposed (Text size = 100 kb)	8.33 seconds	LSB (Text size = 100 kb)	8.33 seconds

Table -1: Size Comparison

PSNR Comparison			
Proposed (Text size = 1 kb)	77.14	LSB (Text size = 1 kb)	77.14
Proposed (Text size = 10 kb)	71.31	LSB (Text size = 10 kb)	77.30
Proposed (Text size = 100 kb)	63.25	LSB (Text size = 100 kb)	63.27

The proposed algorithm can be seen to perform almost as good as LSB both in terms of PSNR and time of execution. However the security of the proposed approach is better. Given that the security of the proposed approach is better it can be said that the proposed approach is better than LSB.

Figure 1 and 2 show outputs before and after execution of our proposed algorithm. It can be seen that there is hardly any visual difference to the naked eye thus showing how good the algorithm is.

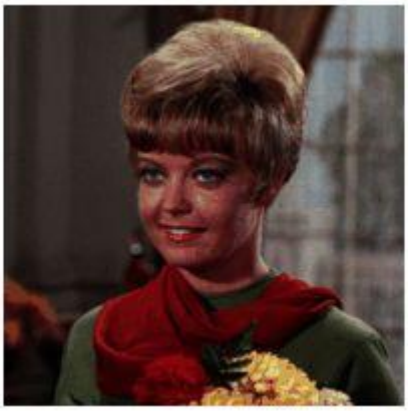

Fig -1: Before algorithm

Fig -2: After algorithm

4. CONCLUSIONS

The proposed approach uses sparse matrix encoding to increase the security of the algorithm. Also it can be seen that the proposed approach did as good as the Least Significant bit algorithm in terms of speed of execution and PSNR value whilst also giving additional security.

Based on the experimental analysis it is safe to say that the proposed algorithm does better than the Least Significant Algorithm and hence for that purpose the proposed algorithm should be preferred.

REFERENCES

[1] Eisenbarth, T. and Kumar, S., 2007. A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, *24*(6).

[2] Gowda, S.N., 2016, September. Innovative enhancement of the Caesar cipher algorithm for cryptography. In *Advances in Computing, Communication, & Automation (ICACCA)(Fall), International Conference on* (pp. 1-4). IEEE.

[3] Peikert, C., 2016. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, *10*(4), pp.283-424.

[4] Costa, D.G., Figuerêdo, S. and Oliveira, G., 2017. Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions. *Cryptography*, *1*(1), p.4.

[5] Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C., 2016, May. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 839-858). IEEE.

[6] Hazay, C., López-Alt, A., Wee, H. and Wichs, D., 2016. Leakage-resilient cryptography from minimal assumptions. *Journal of Cryptology*, *29*(3), pp.514-551.

[7] Hiney, J., Dakve, T., Szczypiorski, K. and Gaj, K., 2015, August. Using facebook for image steganography. In *Availability, Reliability and Security (ARES), 2015 10th International Conference on* (pp. 442-447). IEEE.

[8] Gowda, S.N. and Sulakhe, S., 2016, April. Block Based Least Significant Bit Algorithm For Image Steganography. Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems (ICCSIS-16).

[9] Banik, B.G. and Bandyopadhyay, S.K., 2015, December. Secret sharing using 3 level DWT method of image steganography based on Lorenz chaotic encryption and visual cryptography. In *Computational Intelligence and Communication Networks (CICN), 2015 International Conference on* (pp. 1147-1152). IEEE. [10]

Holub, V., Fridrich, J. and Denemark, T., 2014. Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*, *2014*(1), p.1.

[11] Sedighi, V., Cogranne, R. and Fridrich, J., 2016. Content-adaptive steganography by minimizing statistical detectability. *IEEE Transactions on Information Forensics and Security*, *11*(2), pp.221-234.

[12] Holub, V. and Fridrich, J., 2013, June. Digital image steganography using universal distortion. In *Proceedings of the first ACM workshop on Information hiding and multimedia security* (pp. 59-68). ACM.

[13] Gowda, S.N., 2016, October. Using Blowfish encryption to enhance security feature of an image. In *Information Communication and Management (ICICM), International Conference on* (pp. 126-129). IEEE.

[14] Sedighi, V., Fridrich, J. and Cogranne, R., 2015, March. Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model. In *SPIE/IS&T Electronic Imaging* (pp. 94090H-94090H). International Society for Optics and Photonics.